Faculty of Science, Technology, Engineering and Mathematics
M303 Further pure mathematics

M303

TMA 01 2020J

Mainly covers Book A *Number theory*
Cut-off date 10 November 2020

You will find instructions for completing TMAs in the 'Assessment' area of the M303 website. Please remind yourself of these instructions before beginning work on this TMA. You can submit this TMA either by post, together with a completed TMA form (PT3), to arrive by the cut-off date given above, or electronically, as a single PDF file, using the University's online TMA/EMA service.

Half of the TMA is formative, and the other half is summative. The formative questions are designed to either *extend* your understanding of the topics or *introduce* the topics of later books, while the summative questions place more emphasis on *assessing* your understanding of the topics. Both types of question will be marked by your tutor, but (unlike the summative questions) marks for the formative questions do not count towards your final grade. You should submit your solutions to both sets of questions to your tutor by the cut-off date.

The marks allocated to each part of a question are indicated in the margin.

Although many of the questions on this assignment require numerical answers, the questions invariably carry *method marks*.

In phrasing the questions, we have used the words listed below, each of which should be interpreted as indicated.

prove, show, explain, justify	Clear reasoning and explanation for all steps are called for.
determine, find, devise, calculate, compute	An indication of the method used and all working in arriving at an answer should be given.
deduce	Clear explanation of how one result follows from another is required.
solve	Working must be shown. A numerical answer alone is not sufficient.
evaluate, give, write down, list	Answer suffices. No explanation need be given.
hence	No marks will be awarded for any alternative method.

Copyright © 2020 The Open University

This TMA is based on Book A (Number theory), except for the formative Question 8, which covers the start of Book B.

Part A is **summative**. These questions assess your knowledge of the module. You must not discuss these questions in the forums, and your tutor is not allowed to help you directly.

Part B is **formative**. You should choose two questions to submit to your tutor for feedback, and we suggest that one of these is Question 8 since this will help you with the next TMA.

Doing the formative questions will help you to understand key concepts covered in the text. You are encouraged to discuss these questions in the module forums and with your tutor (who is allowed to help you).

Question 8 is designed to help you with TMA 02. Questions 9 and 10 cover material that is more central to the module, while Question 11 is designed to expand your understanding beyond the core material.

Your tutor will mark all of the answers that you submit. But note that only your marks for Part A count towards your overall continuous assessment score.

Part A Summative

Question 1 – 5 marks

Use mathematical induction to prove that for all integers $n \geq 1$, the number $6^{2n} - 5^n$ is divisible by 31. [*5*]

Question 2 – 6 marks

Use the Euclidean Algorithm to determine integers x and y such that

$$\text{hcf}(1299, 378) = 1299x - 378y.$$

Write down the general solution of this linear Diophantine equation, and find the particular solution in which x takes its least positive value. [*6*]

Question 3 – 11 marks

Let $m = n(n+1)$ be the product of two consecutive integers.

(a) If $m = 6k + r$, where k and r are integers with $0 \leq r \leq 5$, prove that either $r = 0$ or $r = 2$. [*4*]

(b) If $m = 10k + r$, where k and r are integers with $0 \leq r \leq 9$, determine the values of r that are possible. [*4*]

(c) Using the result of part (b), show that the final digit of a triangular number cannot be 2, 4, 7 or 9. [*3*]

Question 4 – 8 marks

(a) Solve each of the following linear congruences.

(i) $3x \equiv 2 \pmod 7$ [*1*]

(ii) $2(2-x) \equiv 5(x-1) \pmod{13}$ [*2*]

(iii) $3x \equiv 4 \pmod{17}$ [*2*]

(b) Determine the least positive integer that satisfies all three of the congruences in part (a). [*3*]

Question 5 – 7 marks

(a) Use Fermat's Little Theorem to find the least positive residue of $12^{74} \pmod{73}$. [*3*]

(b) Prove that $a^{25} \equiv a \pmod{195}$ for every integer a.

(Note that $195 = 3 \cdot 5 \cdot 13$.) [*4*]

Question 6 – 10 marks

Throughout this question, let

$$P(x) = x^3 + 33x^2 + 31x + 10.$$

(a) Write down the degree of P modulo 75. [*1*]

(b) (i) Find all solutions of the polynomial congruence

$$P(x) \equiv 0 \pmod 3.$$ [*2*]

(ii) Find all solutions of the polynomial congruence

$$P(x) \equiv 0 \pmod 5.$$ [*3*]

(c) Use the results of part (b) to find all solutions of the polynomial congruence

$$P(x) \equiv 0 \pmod{75}.$$ [*4*]

Question 7 – 3 marks

An important part of being a mathematician is being able to communicate your ideas and thoughts successfully to other mathematicians. In order to help you to develop this skill over the course of the module, each TMA will contain a short question relating to this theme – you are not required to give long answers.

To start you off, we would like you to do the following.

(a) Watch the informal online session entitled 'M303: Things you need to know' that is linked to from Week 1 on the module website.

(b) Post something in an M303 module forum. To earn full marks, provide either a screenshot of your forum post or directions as to where to find it (giving the forum where posted, thread title, time and date). (If you are not in a position to provide such evidence, contact your tutor for advice.) [*3*]

Part B Formative

Question 8 – 14 marks

This question concerns material from Book B, and relates to Question 2 in TMA 02.

Let G be the set given by $G = \{a + b\sqrt{-7} : a, b \in \mathbb{Z}\}$. Let $+_G$ be the binary operation on G given by

$$(a + b\sqrt{-7}) +_G (a' + b'\sqrt{-7}) = (a + a') + (b + b')\sqrt{-7},$$

for $a, a', b, b' \in \mathbb{Z}$.

Let $H = \{a + b\sqrt{-7} : a, b \in 2\mathbb{Z}\}$ (where $2\mathbb{Z} = \{2n : n \in \mathbb{Z}\}$ is the set of multiples of 2).

(a) Write down the following.
   (i) An identity element of G.
   (ii) An element of H that is not the identity.
   (iii) An element of G that is not in H.
   (iv) The sum (under $+_G$) of your answers to parts (a)(ii) and (a)(iii). [2]

(b) Show that $(G, +_G)$ is a group. [4]

(c) By using the subgroup criterion, or otherwise, show that H is a subgroup of G. [3]

(d) Explain why H is normal. [1]

(e) Write down all four elements of the quotient group G/H, and construct the Cayley table for G/H. [3]

(f) Is G/H cyclic? [1]

Question 9 – 10 marks

This is a very famous puzzle, and you can easily find the solution by searching the web. However, you will gain the most from it if you first attempt to solve it for yourself.

On a rocky planetoid, there are k aliens (where $k \geq 1$) who have blue ears, and the rest of the aliens have green ears. At the start of the puzzle, no alien on the planetoid knows their own ear colour. By rule, if an alien on the planetoid ever discovers that they have blue ears, then they must leave the planetoid at 6 am the following revolution. Each alien on the planetoid knows every other alien's ear colour, but there are no reflective surfaces, there is never any discussion of ear colour, and an alien has no way of determining their own ear colour.

At some point, an outsider arrives, calls together all the aliens on the planetoid, and makes the following public announcement: 'At least one of you has blue ears.' The outsider, furthermore, is known by all to be truthful, and all know that all know this, and so on: it is common knowledge that she is truthful, thus it becomes common knowledge that there is at least one alien who has blue ears.

(a) Assuming that all the aliens on the planetoid are completely logical and that this too is common knowledge, what is the eventual outcome and when does it occur? [2]

(b) Give a proof that your answer to part (a) is correct. [8]

Question 10 – 13 marks

This question introduces ideas that will play a significant role in Books C and E of the module.

For this question you may assume that $\sqrt{p}$ is irrational for all primes p, and that $\sqrt{2}+\sqrt{3}$ is irrational.

A polynomial with integer coefficients of degree n (where $n \in \mathbb{N}$) is an expression $P(x)$ of the form

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_i \in \mathbb{Z}$ for each $i = 0, 1, 2, \ldots, n$, and $a_n \neq 0$.

We say that a real number α is a *root* of a polynomial P if $P(\alpha) = 0$.

(a) Explain why $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{2}+\sqrt{3}$ are not roots of polynomials with integer coefficients that have degree 1. [3]

(b) Let p be a prime number. Find a polynomial $P_p(x)$ with integer coefficients that has degree 2 and for which $\sqrt{p}$ is a root. [1]

(c) Show that the polynomial that you found in part (b) cannot be written as the product of two polynomials with integer coefficients that both have degree 1. [5]

(d) Find a polynomial with integer coefficients for which $\sqrt{2}+\sqrt{3}$ is a root. What is the degree of your polynomial? [4]

Question 11 – 13 marks

This question involves many concepts from throughout Book A, and asks you to investigate congruences with composite moduli.

Let p and q be distinct odd primes.

(a) Prove that an integer x satisfies $x^2 \equiv 1 \pmod{pq}$ if, and only if, x satisfies both

$$x^2 \equiv 1 \pmod{p} \quad \text{and} \quad x^2 \equiv 1 \pmod{q}.$$ [2]

(b) Explain why $x^2 \equiv 1 \pmod{p}$ has exactly two distinct solutions $x \equiv \pm 1 \pmod{p}$. [2]

(c) Use the Chinese Remainder Theorem to explain why $x^2 \equiv 1 \pmod{pq}$ has exactly four solutions. [4]

(d) Solve the congruence $x^2 \equiv 1 \pmod{95}$. [2]

(e) Why does the fact that the congruence in part (d) has four solutions not contradict Lagrange's Theorem in Chapter 4? [3]